Auditdienst Rijk
Ministerie van Financiën

-

Assurancerapport
Monitoringsplan PPS Rijkskantoor de Knoop Utrecht 2017

definitief

Colofon

Titel	Assurancerapport Monitoringsplan PPS rijkskantoor de Knoop Utrecht 2017
Uitgebracht aan	B/CFD Unit HFA
Datum	6 juni 2017
Kenmerk	2017-0000110302

Inlichtingen
Auditdienst Rijk
070-342 7700

Inhoud

Aanleiding opdracht

Het facilitair beheer van het rijkskantoor De Knoop in Utrecht zal worden georganiseerd volgens een Publiek-Private Samenwerking (hierna: PPS). Deze samenwerking betreft aan de ene kant de Belastingsdienst/Centrum voor Facilitaire Dienstverlening (B/CFD) en aan de andere kant de private partij R Creators. Het beheer dient te voldoen aan de kwaliteitseisen zoals die zijn opgenomen in de Outputspecificaties (hierna: OS) en de procedures zoals die in het Monitoringsplan zijn benoemd. R Creators is verantwoordelijk voor de levering van de dienst 'Monitoring' ten behoeve van PPS Rijkskantoor de Knoop. Deze dienst, beschreven in het Montoringsplan, betreft de registratie en afhandeling van de meldingen en periodieke testen die zijn gerelateerd aan de dienstverlening aan de gebouwgebruikers en het beheer van het gebouw zoals dat tot uitdrukking komt in de OS. Het Monitoringsplan is een contractueel document. R Creators heeft de verantwoordelijkheid om die op te stellen.

De implementatie van de processen, maatregelen en het uit het Monitoringsplan is mede afhankelijk van een goedkeurend oordeel hierover door de Audit Dienst Rijk (ADR).

Conclusie

Naar ons oordeel waarborgt *de opzet* van de processen, maatregelen en het beheer van het Registratiesysteem zoals beschreven in het 'Monitoringsplan PPS rijkskantoor de Knoop' (versie 1.0 d.d. 9 mei 2017) en de bijbehorende bijlagen een betrouwbare verwerking van de meldingen en periodieke testen en de rapportage daarover.

Toelichting op de conclusie
De conclusie betreft het feit dat de opzet van de processen etc. een betrouwbare verwerking van de meldingen, periodieke testen en de rapportage waarborgen. De gerealiseerde betrouwbaarheid is afhankelijk van de conforme implementatie van deze maatregelen in en om het Registratiesysteem en de naleving ervan.

1 Verantwoording onderzoek

1.1 Opdrachtformulering

De opdracht bestaat uit 2 gedeelten:

Deel I

De opzet van de dienst Monitoring te toetsen op basis van het Monitoringsplan met de volgende onderzoeksvraag:

"*Waarborgt de opzet van de processen, maatregelen en het beheer van het Registratiesysteem een betrouwbare verwerking van de meldingen en periodieke testen en de rapportage daarover"*

Deel I betreft 2 audits:

- De eerste audit is een audit dat resulteert in een rapport van bevindingen. Dit betreft het concept-Monitoringsplan versie 0.5 (excl. het Projectplan) dat op 14 november 2016 aan de opdrachtgever is aangeboden. Hierover is door ons gerapporteerd met het 'rapport van bevindingen Monitoringsplan PPS de Knoop Utrecht' met kenmerk 2016 – 0000231447 d.d. 21 december 2016. De verwerking van de bevindingen uit het genoemde rapport in versie 0.7 van het Monitoringsplan is in april aanvullend beoordeeld. Daarover is aan de opdrachtgever gerapporteerd op 7 april 2017.

- De tweede audit resulteert in dit onderhavige assurancerapport. De audit betreft het Monitoringsplan (incl. de bijlagen) versie 1.0 dat in mei 2017 is aangeboden aan de opdrachtgever.

Deel II

Het Projectplan, dat is opgenomen in een bijlage bij het Monitoringsplan, te reviewen op de onderbouwing van doorlooptijd, de opzet van de projectorganisatie en de beoogde methodiek. Hierover is gerapporteerd in een brief met het kenmerk 2017-0000016093 d.d. 20 januari 2017.

1.2 Object van onderzoek

Het object van onderzoek van deze audit is het Monitoringsplan (incl. de bijlagen) versie 1.0 d.d. 9 mei 2017. Het Monitoringsplan en de bijlagen zijn beoordeeld voor zover deze het normenkader (zie bijlage 1) betreffen. Procedurele beschrijvingen over bv. reservering van vergaderlocaties zijn niet beoordeeld als onderdeel van de monitoring van de dienstverlening.

1.3 Normenkader

In bijlage 1 staat het normenkader voor de beoordeling van deel I van deze opdracht. Dit normenkader is een best-practice en gebaseerd op andere Monitoringsplannen bij verschillende Publiek Private Samenwerkingen en algemene IT-beheernormen.

1.4 Gehanteerde Standaard

Deze opdracht is uitgevoerd volgens de Richtlijn voor assurance-opdrachten door IT-auditors (NOREA Richtlijn 3000D).

1.5 Verspreiding rapport

De opdrachtgever, B/CFD Unit HFA, is eigenaar van dit rapport.

De ADR is de interne auditdienst van het Rijk. Dit rapport is primair bestemd voor de opdrachtgever met wie wij deze opdracht zijn overeengekomen. In de ministerraad is besloten dat het opdrachtgevende ministerie waarvoor de ADR een rapport heeft geschreven, het rapport binnen zes weken op de website van de rijksoverheid plaatst, tenzij daarvoor een uitzondering geldt. De minister van Financiën stuurt elk halfjaar een overzicht naar de Tweede Kamer met de titels van door de ADR uitgebrachte rapporten en plaatst dit overzicht op de website.

2 Ondertekening

Groningen, 6 juni 2017

Manager Audit
Dienst Rijk

Bijlage 1 Normenkader

Nr.	Norm
A	**Proces- en applicatiecontrols**
1	Rollen en autorisaties
1.1	Organisatorische functiescheidingen zoals belegd in de organisatie dienen te zijn gewaarborgd door middel van autorisaties in de applicatie.
1.2	Periodiek worden toegekende autorisaties op actualiteit (uitdiensttredingen, functiewijzigingen, geen gebruik, aangepaste rechten) gecontroleerd en bevestigd door het management.
1.3	Autorisaties dienen te zijn gebaseerd op een role-based toegangsconcept waarbij gebruikers behoren tot rollen en aan rollen autorisaties zijn toegewezen.
1.4	Autorisatie op basis van need to know principe: Gebruikers dienen uitsluitend toegang te hebben tot programma's (rollen) die zij ten behoeve van hun werkzaamheden nodig hebben.
1.5	Administrator rechten zijn beperkt toegekend.
1.6	De autorisatiematrix dient te zijn gedocumenteerd, actueel te zijn en door de eigenaar van de applicatie te zijn geautoriseerd.
1.7	Aanvragen van autorisaties c.q. aanpassen van autorisaties verloopt via een formele procedure en pas na goedkeuring worden rechten toegekend.
1.8	Mutaties in autorisaties dienen te worden gelogd zodat wijzigingen achteraf herleidbaar en controleerbaar zijn (audittrail).
1.9	Wachtwoorden dienen sterk te zijn en periodiek te worden gewijzigd (password policy).
2	Beheren meldingen
2.1	Incidenten, storingen en helpdeskverzoeken (meldingen) dienen betrouwbaar (juist, tijdig en volledig) te worden geregistreerd.
2.1	a -Het gehele systeem dient te zijn voorzien van een gesynchroniseerde standaarddatum/tijdsaanduiding gebaseerd op standaard UTC.
2.1	b - Meldingen mogen niet onvolledig kunnen worden ingevoerd.
2.1	c - Meldingen worden geclassificeerd en geprioriteerd conform de afspraken in de Outputspecificaties.
2.1	d - Meldingen zijn doorlopend genummerd.
2.1	e - Indien de koppeling tussen de afzonderlijke registratiesystemen (indien van toepassing) niet functioneert, is er een workaround waarbij de betrouwbare verwerking van de meldingen is getoetst.
2.2	Incidenten, storingen en helpdeskverzoeken (meldingen) dienen op een betrouwbare wijze en conform de opgestelde procesgang en workflow te worden afgehandeld.
2.2	a - Gegevens die van invloed zijn op de "afrekening" mogen niet tussentijds gecorrigeerd kunnen worden.
2.2	b - Wijzigingen in gegevens die mogelijk van invloed zijn op de "Afrekening" (bijv. on hold, niet ontvankelijk of facilitair) dienen achteraf inzichtelijk te zijn.
2.2	c - Meldingen kunnen niet worden verwijderd.
2.2	d - meldingen worden bewaakt op tijdige afhandeling.
2.3	De betrouwbaarheid (juist-, tijdig- en volledigheid) van het gereedmeldingstijdstip dient te zijn gewaarborgd.
2.3	a - melding dient op juiste tijdstip te worden gereed gemeld (systeem tijd).
2.3	b - oplossing van de melding dient te worden gedocumenteerd.
2.3	c - indien de koppeling tussen de afzonderlijke registratiesystemen (indien van toepassing) niet functioneert dient in de workaround getoetst te worden dat het gereedmeldingstijdstip juist is en de afmelding naar de melder te zijn opgenomen.
2.4	Het plannen van de periodieke testen (als onderdeel van de PPS-overeenkomst), het uitvoeren daarvan alsmede de betrouwbare vastlegging dienen te zijn gewaarborgd.

Nr.	Norm
3	Interfaces met andere systemen
3.1	koppeling GBS: Via het gebouwregistratiesysteem worden meldingen ontvangen. De betrouwbare (juiste, tijdige en volledige) registratie van deze berichten in het Registratiesysteem dient te zijn gewaarborgd.
3.1	a - Koppeling GBS: De inleesfunctie dient (na uitval of crash) herstartbaar te zijn zonder fouten (geen verstoring betrouwbaarheid). Fouten bij het inlezen worden herkend en opgelost.
3.1	b - De inregeling van het GBS wordt intern getoetst.
3.1	c - Koppeling GBS: Handmatig corrigeren c.q. invoeren van een GBS melding is alleen mogelijk voor daartoe geautoriseerde medewerkers en de handmatige vastlegging is als zodanig herkenbaar.
3.1	d - Koppeling GBS: Systeemklokken GBS en het Registratiesysteem dienen te zijn gesynchroniseerd.
3.1	e - Koppeling GBS: De gegevens vanuit het GBS moeten de informatie leveren die een juiste classificatie mogelijk maakt.
3.2	koppeling GBS: Via het gebouwregistratiesysteem worden meldingen ontvangen. De betrouwbare (juiste, tijdige en volledige) verwerking van deze berichten in het Registratiesysteem dient te zijn gewaarborgd.
3.3	koppeling GBS: Via het gebouwregistratiesysteem worden meldingen ontvangen. De betrouwbare (juiste, tijdige en volledige) afmelding van deze berichten in het Registratiesysteem dient te zijn gewaarborgd.
3.4	Koppeling GBS: De betrouwbaarheid van de koppeling tussen het GBS en het Registratiesysteem dient achteraf controleerbaar te zijn.
3.5	Koppeling intranet: Gebruikers voeren meldingen via het intranet portal. De betrouwbare (juiste, tijdige en volledige) verwerking van de meldingen in het Registratiesysteem dient te zijn gewaarborgd.
3.6	Inkomende e-mail: Gebruikers sturen e-mail berichten en de betrouwbare (juiste, tijdige en volledige) registratie van deze berichten in het Registratiesysteem dient te zijn gewaarborgd.
3.7	Uitgaande e-mail: Na registratie van de melding ontvangt de(gebruiker(melding) een emailbericht met bevestiging. De betrouwbaarheid (juistheid, tijdigheid en volledigheid) van deze email berichten dienst te zijn gewaarborgd.
4	Rekenregels
4.1	De relatie tussen de outputspecificatie en de kortingsberekeningregels moet eenduidig zijn vast te stellen.
4.2	Betrouwbaarheid van kortingsberekeningsregels voor alle Outputspecificaties dient te zijn gewaarborgd.
4.3	Betrouwbaarheid van het geautomatiseerde kortingsberekeningsmechanisme moet zijn gewaarborgd.
5	Onderhoud en beheer
5.1	Er is een actuele en door het management goedgekeurde procedure vastgelegd voor het wijzigen van Stamgegevens c.q. gegevens die van invloed zijn op de te berekenen kortingen.
5.2	De procedure voor wijzigen van stamgegevens is in overeenstemming c.q. sluit aan op contractuele afspraken met de belastingdienst.
5.3	Alleen geautoriseerde medewerkers kunnen wijzigingen in stamgegevens en rekenregels doorvoeren.
5.4	Mutaties op stamgegevens die direct of indirect van invloed kunnen zijn op de betrouwbaarheid van de kortingsberekening (o.a. meldingscategorie, kortingen en toegestane hersteltijden) dienen te worden gelogd zodat wijzigingen achteraf herleidbaar en controleerbaar zijn (audittrail).
5.5	Betrouwbaarheid van de ruimteclassificatie dient te zijn gewaarborgd.
5.6	Betrouwbaarheid van de normwaarde signalering dient te zijn gewaarborgd.
5.7	Betrouwbaarheid van de in het Registratiesysteem vastgelegde meldingen en classificatie dient te zijn gewaarborgd.
B	**IT General Controls**
6	Logische toegangsbeveiliging
6.1	Remote access is beveiligd door middel van user-ids en wachtwoorden (eventueel ook op basis van tokens).

Nr.	Norm
6.2	Remote datacommunicatie (technische verbinding tussen het Registratiesysteem en server) is beveiligd (VPN, HTTPS).
7	Continuïteit
7.1	Continuïteitsmaatregelen (back-up, recovery, uitwijk etc.) zijn in overeenstemming met de contractueel overeengekomen beschikbaarheideisen.
7.2	De continuïteitsmaatregelen worden periodiek getest. Op basis hiervan wordt het plan geëvalueerd en indien nodig verbeteringen getroffen.
7.3	Er is een actueel, gedocumenteerd en door het management geaccordeerd plan voor continuering van de dienstverlening en handhaving van het service niveau.
8	Wijzigingsbeheer
8	Wijzigingen in (1) de programmatuur, in (2) de applicatie, in (3) de database en in (4) het onderliggende platform dienen op een gecontroleerde en gedocumenteerde manier plaats te vinden.
8.1	Er is een wijzigingsprotocol.
8.2	Wijzigingsverzoeken en de afhandeling daarvan is gedocumenteerd en voor ieder wijzigingsverzoek is (achteraf) een audittrail beschikbaar.
8.3	Wijzigen dienen voor in gebruik name te worden getest.
8.4	Gebruikers dienen in de test te worden betrokken.
8.5	Testscenario's worden gehanteerd en testbevindingen worden gedocumenteerd.
8.6	Wijzigingen dienen alleen met toestemming van de interne eigenaar van de applicatie te worden geïmplementeerd in de productieomgeving.
8.7	Gebruikers worden geïnformeerd over aard van de wijziging en het moment van implementatie.
8.8	Na de implementatie van wijzigingen vindt aanvullende monitoring plaats op het correct werken van de applicatie.
9	Uitbestede werkzaamheden (indien van toepassing)
9.1	Indien aan de applicatie gerelateerde systeembeheer en/of applicatie ontwikkelingswerkzaamheden zijn uitbesteed dan dienen daaraan contractuele afspraken ten grondslag te liggen (Service Level Agreements).
9.2	In de contractuele afspraken dient minimaal het dienstenniveau te zijn gedefinieerd.
9.3	De dienstverlener dient periodiek te rapporteren over het behaalde diensten niveau.
9.4	Rapportages over het behaalde dienstenniveau dienen te worden besproken tussen de partijen en indien van toepassing dienen verbeteracties te worden geïnitieerd.

Auditdienst Rijk
Postbus 20201
2500 EE Den Haag
(070) 342 77 00